# lokunlola

Cloud-Virtualization-Project

**## Automated ELK Stack Deployment**

The files in this repository were used to configure the network depicted below.

***https://github.com/mrlaokunlola/lokunlola/blob/main/Network%20diagram.png***

These files have been tested and used to generate a live ELK deployment on Azure. They can be used to either recreate the entire deployment pictured above. Alternatively, select portions of the **yml and config** file may be used to install only certain pieces of it, such as Filebeat.

* **My first playbook**
* **Hosts**
* **Ansible Configuration**
* **Ansible ELK Installation and VM Configuration**
* **Filebeat Config**
* **Filebeat Playbook**
* **Metricbeat Config**
* **Metricbeat Playbook**

This document contains the following details:

* **Description of the Topology**
* **Access Policies**
* **ELK Configuration**
  + **Beats in Use**
  + **Machines Being Monitored**
* **How to Use the Ansible Build**

**### Description of the Topology**

The main purpose of this network is to expose a load-balanced and monitored instance of DVWA, the D\*mn Vulnerable Web Application.

Load balancing ensures that the application will be highly **functional and avaulable** in addition to restricting **traffic** to the network.

What aspect of security do load balancers protect? What is the advantage of a jump box? \_

**Load balancers add resiliency to the network by ensuring availability of the system in a case of disaster, or service disruption.**

**Jump box technology on the other hand ensures a secure and closed network by being a gate way to a protected server. It ensures the limitation of number of connections, ensures the restriction IP addressing. You must connect to the jumpbox before gaining access to the server.**

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the **networks** and system **logs**.

- \_TODO: What does Filebeat watch for? **Filebeat monitors the log files, collect logs events, and forward the, to logstash for indexing.**

- \_TODO: What does Metricbeat record? **Metricbeats forwards metrics and stats to logstash for analyzing.**

The configuration details of each machine may be found below.

**| Name | Function | IP Address | Operating System |**

**|----------|----------|------------|------------------|**

**| Jump Box | Gateway | 10.0.0.4 | Linux |**

**| Web-1 | Ubuntu | 10.0.0.5 | Linux |**

**| Web-2 | Ubuntu | 10.0.0.6 | Linux |**

**| DVWA | Ubuntu | 10.0.0.7 | Linux |**

**### Access Policies**

The machines on the internal network are not exposed to the public Internet.

Only the **Jump box provisioner machine** can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

**- Workstation MY Public IP through TCP 5601**

Machines within the network can only be accessed by **Workstation and jumpbox through SSH Jump-BOX.**

- \_TODO: Which machine did you allow to access your ELK VM? What was its IP address?\_**Jump-Box-Provisioner IP:10.1.0.4 via SSH PORT 20, Workstation MY Public IP through TCP 5601**

A summary of the access policies in place can be found in the table below.

**| Name | Publicly Accessible | Allowed IP Addresses |**

**|----------|---------------------|----------------------|**

**| Jump Box | Yes | 20.248.168.69 |**

**| Web-1 | No | 10.1.0.4 on SSH 22 |**

**| Web-2 | No | 10.1.0.4 on SSH 22 |**

**| DVWA | No | 10.1.0.4 on SSH 22 |**

**| ELK | No | Workstation MY PublicIP Using TCP5601|**

**### Elk Configuration**

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because...

- \_TODO: What is the main advantage of automating configuration with Ansible?\_**Lightweight technology, easy deployment and automation.**

The playbook implements the following tasks:

- \_TODO: In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.\_

**SPECIFY A DIFFERENT GROUP OF MACHINE**

* **Name: Configure ELK VM with docker**
* **Hosts: elk**
* **Become: true**

**Tasks:**

**INSTALL DOCKER.io**

* **Install docker.io**
* **Apt:**

**Update cache:yes**

**Force\_apt\_get:yes**

**Name: docker.io**

**State: present**

**INSTALL PYTHON-PIP**

* **Name: install python3-pip**
* **Apt:**

**Force\_apt\_get: yes**

**Name: pythong3-pip**

**State: present**

**# use pip module (it will default to pip3)**

**Name: install docker module**

**Pip:**

**Name: vm.max\_map\_count**

**Value: ‘262144’**

**State: present**

**Reload: yes**

**DOWNLOAD AND LAUNCH ELK DOCKER CONTAINER**

* **Name: download and launch a docker elk container**

**Docker\_container:**

**Name: elk**

**Image:**

**State: started**

**Restart:policy: always**

**PUBLISH PORTS**

* **Publish\_ports:**

**5601: 5601**

**9200: 9200**

**5044: 5044**

The following screenshot displays the result of running `docker ps` after successfully configuring the ELK instance.

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, text, application, email

Description automatically generated

**### Target Machines & Beats**

This ELK server is configured to monitor the following machines:

- \_TODO: List the IP addresses of the machines you are monitoring\_

* **Web-1:10.1.0.5**
* **Web-2: 10.1.0.6**
* **DVWA: 10.1.0.7**

We have installed the following Beats on these machines:

- \_TODO: Specify which Beats you successfully installed\_

**Filebeat:**

**./filebeat setup**

**./filebeat -e**

**Metricbeat**:

**./metricbeat setup**

**./metricbeat** -**e**

These Beats allow us to collect the following information from each machine:

- \_TODO: In 1-2 sentences, explain what kind of data each beat collects, and provide 1 example of what you expect to see. E.g., `Winlogbeat` collects Windows logs, which we use to track user logon events, etc.\_

**Filebeat will be used to collect logs**

**Metricbeat will be used to monitor VM stats : memory, network, CPU**

**### Using the Playbook**

In order to use the playbook, you will need to have an Ansible control node already configured. Assuming you have such a control node provisioned:

SSH into the control node and follow the steps below:

- Copy the **\_\_\_yml\_\_ file to ansible folder**

- Update the **config file to include remote users and ports**

- Run the playbook, and navigate to **Kibana** to check that the installation worked as expected.

\_TODO: Answer the following questions to fill in the blanks:\_

- \_Which file is the playbook? Where do you copy it?\_

- \_Which file do you update to make Ansible run the playbook on a specific machine? How do I specify which machine to install the ELK server on versus which to install Filebeat on?\_

**/etc/ansible/hosts file (ip of the VM)**

**Specify two separate groups in etc/ansible/hosts file**

- \_Which URL do you navigate to in order to check that the ELK server is running?

**http://ip:port//app/kibana**

\_As a \*\*Bonus\*\*, provide the specific commands the user will need to run to download the playbook, update the files, etc.\_

A screenshot of a computer

Description automatically generated with medium confidence

Text

Description automatically generatedText

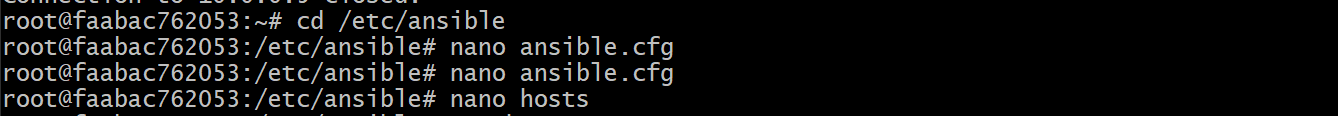
Description automatically generated

Text

Description automatically generated

Text

Description automatically generated



Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence

Text

Description automatically generated